GvIB Expert Letter – September 2006
ISSN 1872-4884, Volume 1 – No. 3

Security Principles: Information security on the management agenda

Aart Jochem

Alex Bewier

Lucien Bongers

Lex Borger

Henk Coenen

Ben Elsinga

Erik Jonkman

Renato Kuiper

Martijn Oostdijk

Daan Rijsenbrij

André Smulders

The organisation of information technology has got through to the management agendas of most organisations today. New demands in areas such as governance and organisational control call for information security to be on the same agenda. At the same time, more information is traded between organisations and trust and security has become fundamental issues. Too often random security solutions are introduced whereby security experts work independently. The different disciplines within an organisation are in need of a common framework in which matters such as the corporate vision, information architecture and security are connected and maintained. Security Principles offer a primary handle to getting a grip on this complex situation.

Page

🖱 http://www.gvib.nl/

✉ expertbrief@gvib.nl

1. Introduction Security Principles

The importance of security and privacy increases in an era where IT becomes more and more embedded in our business procedures, in our society and in our personal lives. **One of the reasons that e-business is not larger and more encompassing is the lack of sufficient security.** Non-repudiation of transactions, outsourcing, and security, all play important roles. Some relevant questions are: 'how do I remain in charge?' and 'is it safe?'

Security and privacy are two sides of the same coin. Where security is mentioned, privacy is also inferred.

Often diverse security solutions are introduced which are more or less independent of the information architecture, whilst coherence is key to maintaining a grip on the complexity as a whole. Integrating security demands into the information architecture afterwards leads many enterprises into difficulties. This is visible in security measures that do not comply with the fundamental architectural principles, which results in the need for extra measures in order to implement the solution. The consequences are barely incalculable but can, in many ways, cause breakdown, inconsistency and unnecessary complexity. Applications becoming less secure and client frustration due to a misfit to human measure are only some of the problems that may occur.

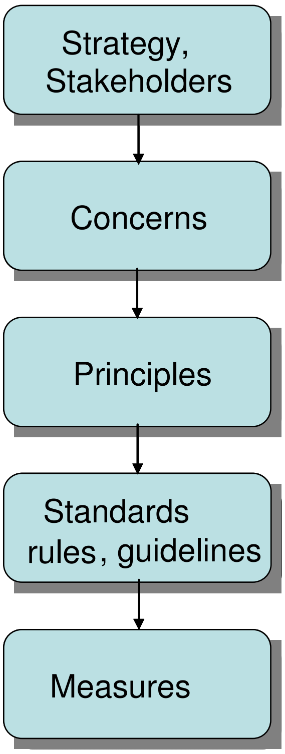
The approach of security experts when designing security measures is guided by the following questions:

- Why is security important? Answering this question provides insight into the organisation, the context and the organisational goals. At this stage basic principles are found, for instance regarding impact on the user (perception), costs, availability and compliance with the law, rules and regulations.
- What is to be secured and against what? Nearly all frameworks for information security in use (CobiT, Code of Practice for Security Management, VIR A&K) evolve from an inventory of resources and threats to create risk profiles.
- What are appropriate concepts? The architectural principles conceived in this stage provide avenues of solutions and offer a structure in which the measures can be implemented.
- How are the concepts implemented? Which standards and guidelines are utilised?
- With what is the information security implemented and supported?

Just like digital architects, security experts make global designs based on principles, rules, standards and guidelines in order for technical designers to detail the work. Strangely enough, in many enterprises security and information architecture are not integrated.

1.1 The Role of Principles

Principles are guiding statements related to essential decisions, a fundamental idea meant to fulfil the general aim. The aim stems from a **concern** related to the company strategy. Concerns indicate which aspects can hamper the business, which problems could arise. Principles express what is important to an organisation, what it believes in and demarcate the design area. They are the mainsprings for organisational behaviour and therefore have influence on the information architecture. For this reason, good principles are comprehensible to all within the organisation.



Principles determine the **course** in setting up and working out the information architecture and function as a **testing framework** to judge this architecture and the design of the information systems.

Today concerns are posed to organisations bij **corporate governance laws** and **behavioural codes,** for example Sarbanes-Oxley in the USA and the Code Tabaksblat in the Netherlands. These concerns are too often addressed by new IT-solutions so that feedback to the client in the organisation is tiresome or incomplete. Definitions of principles can aid this. Legislation seldom provides for universal principles (the Dutch privacy law is an exception to this).Principles help in this by providing the foundation of how laws are upheld.

Are security principles different from architectural principles?
With deploying IT to attain strategic goals, specific concerns about trust, integrity and availability of information will be assessed. These concerns need to be addressed by principles. But the role and place of security principles in the security architecture is equal to those of principles in the information architecture, only the concerns they address are different. Can we then speak of security architecture? Security is a quality aspect of the processing of information and therefore an aspect of the information architecture. Information architecture is not complete without addressing security. Ideally, Security Architecture should not be a separate part of an organisation or project. The IT-architect must assess all user aspects of the systems and the information and will then hire *security experts.* There are no fire protection architects, are there?

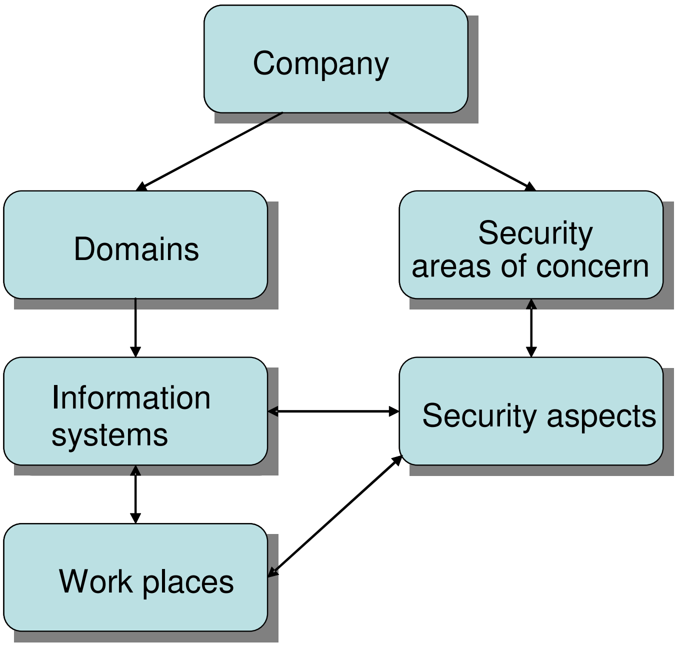
As long as security is separate from the information architecture or is later added independently as an area for special attention, security architectures will be necessary. But with the maturation of the information architecture, security will become an integral part of business procedures and information systems.

2. RESEARCH QUESTIONS

This expert letter attempts to induce a holistic approach, with the goal being to promote the integration of security issues and information architecture. This leads to the following research questions:

- Which security aspect areas can generally be distinguished?
- Which security principles are usually formulated in these security aspect areas?
- How security principles are individually put in order?
- What is the possible effect/impact of security principles?
- How are the correct security principles chosen in a specific situation?

3. SECURITY FOCAL POINTS AND ASPECTS



Relations between architectural topics and security topics

The first question, concerning security focal points has no simple answer. The perspective from which the organisation is studied determines the choice. Frameworks such as CobiT and the Code of Practice offer standard perspectives for Information Security. These frameworks form a set of policy statements, procedures and technology that standardises the approach of information security within an organisation. Examples of focal points are physical security, business continuity, logical security, personnel, etc. It is important to assess the concerns stemming from strategy or from key figures in the organisation. For example, how does one protect a firm from intentional criminal actions or from interruption of business processes? Or, can security measures improve the trust between partners in a business chain?

Information Security offers a range of assessments of security aspects. The Code of Practice for Information Security Management is based on the aspects of *availability, integrity and confidentiality* of information. CobiT, partly geared to assessment of information systems, mentions the criteria, *effectiveness, efficiency, confidentiality, integrity, availability, compliance* and *reliability* of information as more general aspects of the information provision.

4. CHARACTERISTICS OF GOOD SECURITY PRINCIPLES

Setting up security principles occurs in the first phase of an architectural course, such as setting up an information security policy or choosing an avenue of solution. When more than one course is being carried out on different partial aspects of the architecture, it is important to make a connection between the principles in these courses. In order to set up good principles the concerns must be clarified. After which, once the organisation and context have been studied, the security principles can be established. Security principles are hidden in existing policy documents and procedures, and in the behaviour and beliefs of the management of the organisation. During a search a long list of principles will soon emerge, mixed with guidelines, design demands and assumptions of information systems.

A good principle has the following characteristics:

- It is a motivation for behaviour in an organisation;
- It is an underlying starting point that influences the information architecture;
- It is easy to communicate; the more strategic the principle, the simpler it is to communicate;

- It is robust:
    - It is difficult to crack;
    - It does not change its meaning in another context;
    - It is durable;
- It is recognised and supported by management.

Principles are present at all levels, strategically, tactically and operationally. They force you to explain deviations. Principles will often bring about contradictions and so cause considerations and prioritising. Priorities help to determine how to deal with these contradictions: a principle with a higher priority prevails over a principle with a low priority. Some principles are recognised as starting points but have a low priority. They are "nice-to-have" principles.

Principles must be put down in writing: they form a testing framework for architecture and implementation of information security measures and are the link to the concerns. Aside from this it is easier to communicate when the principles are written in clear language. The article *Architecture Principles* by the Open Group [8] provides a useful format for this.

5. Ordering Security Principles

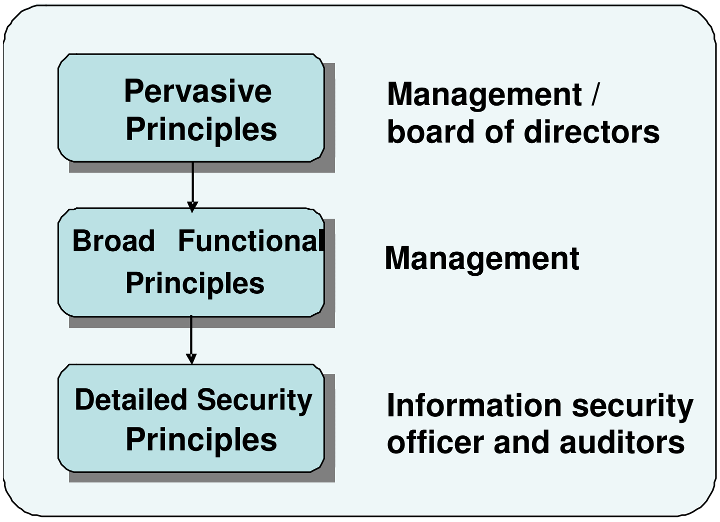
Together with the maturing of the security professionalism, general utilisable principles, patterns[1] and controls[2] are accumulated and documented. The levels of abstraction differ and thus creating a necessity for ordering. There are several ways in which to bring about ordering, some of which are discussed below.

General accepted information security principles (GAISP)

The framework of GAISP evolved after the US National Research Council publicised recommendations for the improvement of information security in the report "Computers at Risk". GAISP started as GASSP (general accepted system security principles)'.

The basis for GAISP consists of three categories of principles [2]:

- Pervasive principles (PP's) or fundamental principles are based on controlling an organisation and providing guidelines on a strategic level. These are 9 basic principles that barely change in the course of time. Examples of pervasive principles are the *accountability principle;* about the accountability and responsibilities in the domain of information security; the *proportionality principle* concerning the balance of measures and risks and the *equity principle* about respecting individual rights.


Pervasive Principles
Management / board of directors
Broad Functional Principles
Management
Detailed Security Principles
Information security officer and auditors

[1] Information security patterns are standard solutions for common problems in a specific context[14]

[2] Information security controls are measures to control confidentiality, availability and integrity of information and information systems

- Broad functional principles (BFP's) are more detailed and define recommended tactics from management's perspective. There are 14 defined BFP's. A BFP supports one or more pervasive principles. BFP-1, the security policy, supports them all. Other BFP's concern accountability, information management, access control, etc.
- Detailed security principles (DSP's) deliver specific and detailed approaches, written for the security and audit professionals and geared to operational security and risk management. These principles provide methods to realise the BFP's. There are many DSP's that support a BFP. An example is the use of one-time passwords, to help realise the BFP access control and to support the PP proportionality.

The principles and ordering that the GAISP provides are well thought-out and substantiated. An objection to ´standard´ principles is that there is no correlation with the concerns; the principles are still *best practice*. With GAISP this is sidestepped as the principles are related to each other on three levels and support each other as well. The use of a detailed principle can be traced back to a pervasive principle, so that the impact of changes can be followed. The pervasive principles are so fundamental and clearly worded that the link with organisational concerns is easily identified. Detailed security principles however, are still being developed.

Security principles according to Elsinga/Hofman

In their article [4] Elsinga and Hofman describe three sorts of principles:

- Mindset principles provide the direction of thought for security in an organisation and are used to formulate security strategies;
- Architecture principles indicate the avenues of solutions when designing security controls;
- Execution principles indicate how to handle complex changes.

This layout is interesting because they approach information security principles from the perspective of the designer and the effect of the security principles. A direct connection between the three layers is not a necessity, but there must be harmony.

An **example** for illustration:

> A viable concern for an organisation connected to the Internet is the threat of computer systems being broken into. A formulated security principle is protecting the front door (the internet connection) from unauthorised access ("fortress mentality"). As a standard architectural principle, perimeter security will be chosen, which is carried out with a central firewall.
>
> After the publication of statistics about internal threats the concern shifts: it is no longer merely the threat of breaking in from the outside, but now also from within. Related architectural principles are compartmentalising and object .The Jericho-forum even discusses *de-perimeterisation*, to illustrate how deeply the perimeter security principle is anchored.

6. SETTING UP SECURITY PRINCIPLES

Setting up security principles is largely an interactive process. Because they must 'live' in an organisation they cannot originate from the information security expert alone. But he can put them in order. The principles address the concerns of management. This must also be the starting point: what is known about mission and design of information technology, what is stated in policy and architectural documents.

It is highly recommended that applied principles, especially principles on the level of pervasive or mindset principles, be discussed with senior management and the board and the management of the IT-organisation. For this, information security must have been brought to management's agenda. It is also important to make note of wording. Formulate sharp and clear and avoid technical phrases and jargon. Allow management to assist with prioritising principles.

The principles must also be tested whether they are related to living concerns in the organisation and meet the criteria for good principles. The above-mentioned standard principles provide a grip for developing the pervasive or mindset principles to more detailed principles. The GAISP and the Elsinga/Hofman layout provide a good grip. It is important to pay attention to the relationship between principles and concerns. The standard principles provide a solution for oft occurring problems. They form a handy checklist and can speed up the process, but the relationship with the concerns must be brought about personally.

7. Conclusions and follow-up

- There is still a lot of difference between definitions of terms and also the way in which security principles are applied varies. There are many ideas, but it is clear that we have not yet mastered this area of the profession. There still seems to be a gap between theory and practice: how can information security principles be applied in day to day business?
- Security principles are difficult to grasp and must be set up with careful attention. An important characteristic of principles is that they form the basis of behaviour within an organisation. When the principles are clear, they are of great value to an organisation in the design of balanced measures.
- Management is still not involved enough in setting up security principles. In this area there is much work to be done. A correct approach and the clear formulation of principles from business perspective are important aspects of this process.
- There is a dependence between the maturity of an information security organisation and its information security principles. As quality, reliability and governance improve, starting points will change and principles will be applied more formally. There is an optimum: in extreme cases, chaos will reign and few principles will count, while too many principles impede the flexibility of an organisation.
- The fact that generic security principles exist indicates that a separate security stream exists in the information architecture. It is important to recognise this and to work on fine-tuning the streams.

8 *How further?*

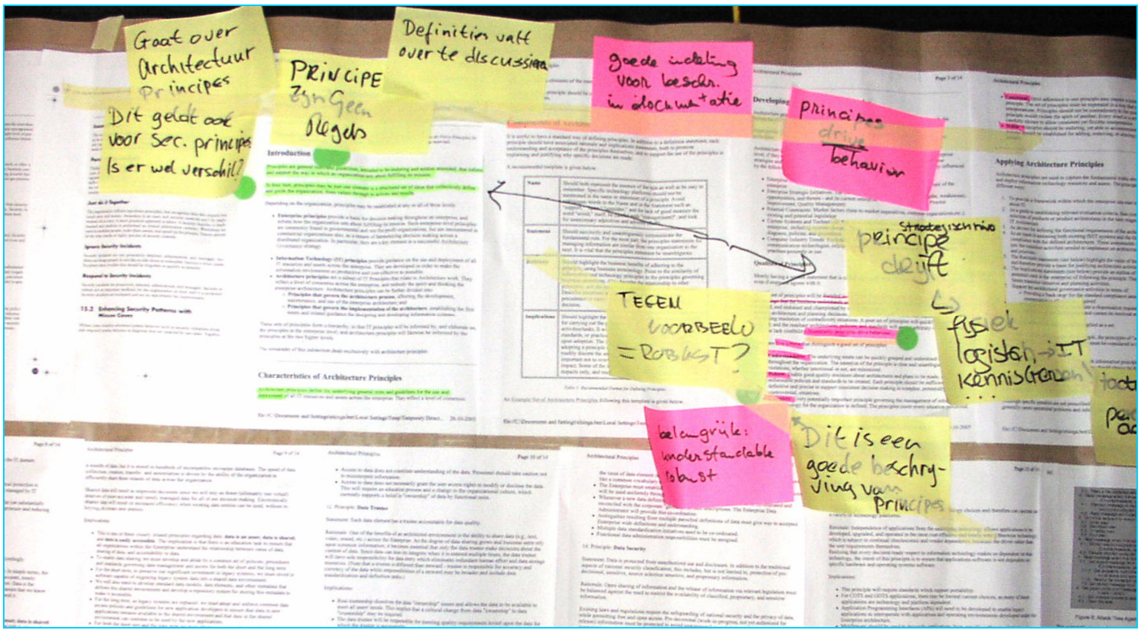
Due to the complexity of the material and the restricted time frame in which this subject can be discussed, many questions remain unanswered:

- What definitions are there about information security principles and what relationships exist?
- Which frameworks address information security principles, which is the best to employ?
- Who owns information security principles, the business or the security team?
- Are information security principles described on an organisational level, domain level or a combination of the two?
- How is the relationship today between digital and security architects and how will this shift with time?

This article is a first attempt to prompt a broader discussion in which the input from as many relevant persons as possible is desired. The expert group therefore invites you to respond. We would also like to refer you to the thesis written by Lucien Bongers on this subject which will be released in 2006*: http://www.student.ru.nl/l.bongers/onderzoek.htm*

We would like to thank the **Information Security Practitioners Association** (www.gvib.nl) for sponsoring the translation of this paper from Dutch to English.

If you like this paper or if you have important remarks, please send and e-mail to expertbrief@gvib.nl


Gaat over Architectuur Principes
Dit geldt ook voor Sec. principes Is er wel verschil?
PRINCIPE Zijn Geen Regels
Definitie valt over te discussiëren
goede indeling voor beschr. in documentatie
principes drive behavior
strategisch niveau principe drijft
fysiek logistiek→IT kennisGeneratie ...
TEGEN VOORBEELD =ROBUST?
belangrijk: understandable robust
Dit is een goede beschrijving van principes

GvIB Expert Letter under construction

References

In order to realise this expert letter on *Security Principles* the workgroup consulted the following literature:

[1] Sietse Overbeek, Sergej van Middendorp and Daan Rijsenbrij, *De Digitale Werkruimte, een nieuw architectuurartefact*, June 2005

[2] International Information Security Foundation, *GASSP (Generally Accepted System Security Principles)*, June 1999

[3] US National Security Agency, *Defense in Depth*, June 2001

[4] Ben Elsinga, Aaldert Hofman, *Security Principles,* pattern paper submitted for EuroPlop 2003.

[5] Bert Snel, *Informatie Beveiliging Opzet & Bewustzijn,* Siemens white paper, June 2005

[6] Dan Blum, *Security and Risk Management Strategies Reference Architecture Principles*, Burton Group, jan 2005

[7] Lee Hopkins, *Dialogue: The Four Dialogic Principles For Successful Communication*, http://www.b2bhints.com/biz/2004/12/dialogue_the_fo.html

[8] Open group, *Architecture Principles*, http://www.opengroup.org/architecture/togaf8-doc/arch/p4/princ/princ.htm

[9] Lex Borger, *Presentatie Security Architectuur Principes*

[10] Gary Stoneburner, Clark Hayden, Alexis Feringa*, Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* NIST Special Publication 800-27 Rev A

[11] Bruce Schneier, *Modeling security threats*, in Dr. Dobbs Journal, December 1999

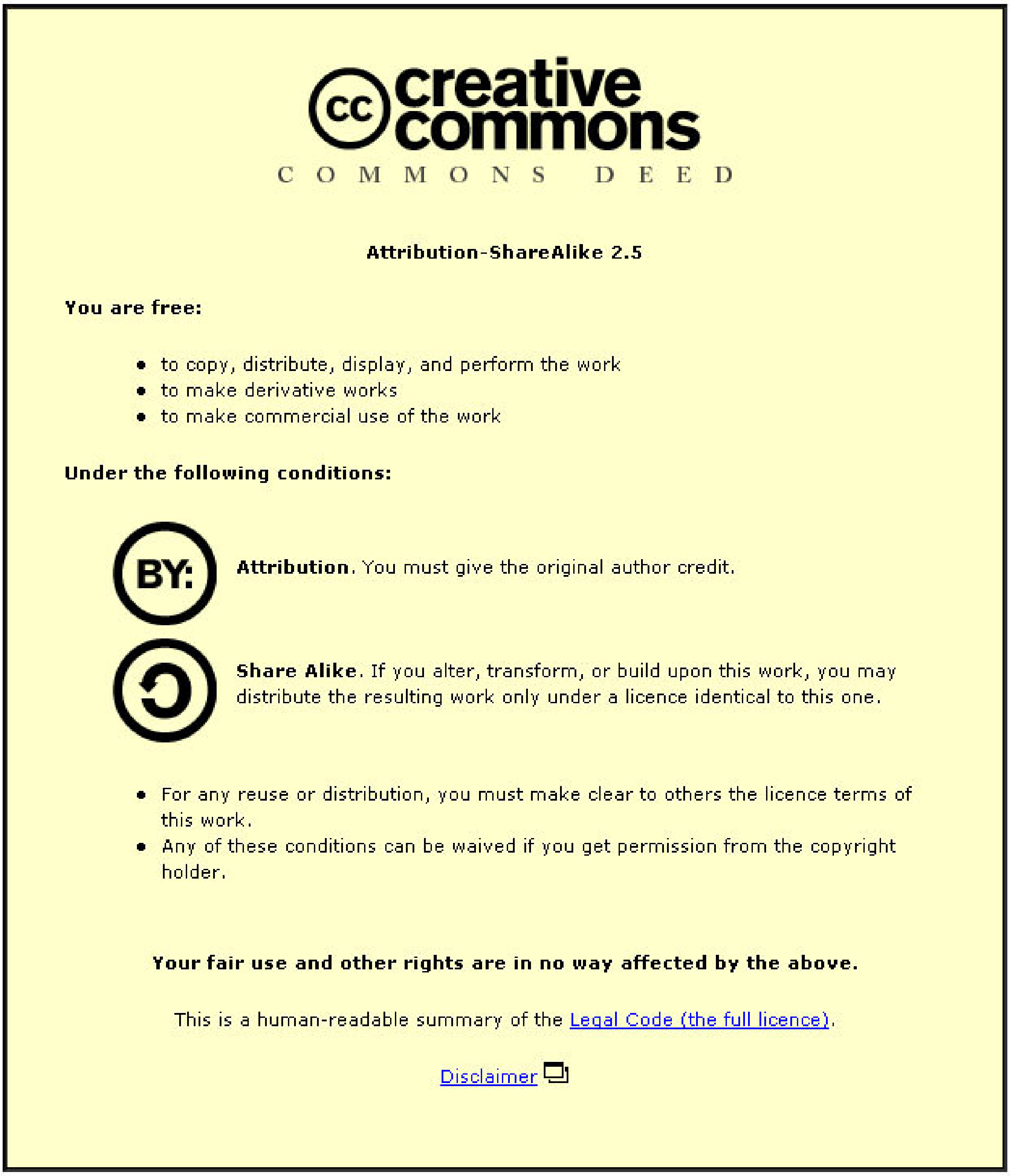
[12] Carl E. Landwehr, *Computer Security*, Springer-Verlag, July 2001

[13] M. Schumacher, *Foundations of Security Patterns*, from Security Engineering with Patterns, Springer-Verlag, 2003

[14] Supplement of the *Security Patterns boek,* http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470858842.html

10 APPENDIX: LICENSE FOR THIS PUBLICATION

This expert letter has been published according to the following license:
http://creativecommons.org/licenses/by-sa/2.5/



creative commons

COMMONS DEED

Attribution-ShareAlike 2.5

You are free:

- to copy, distribute, display, and perform the work
- to make derivative works
- to make commercial use of the work

Under the following conditions:

BY: **Attribution**. You must give the original author credit.

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a licence identical to this one.

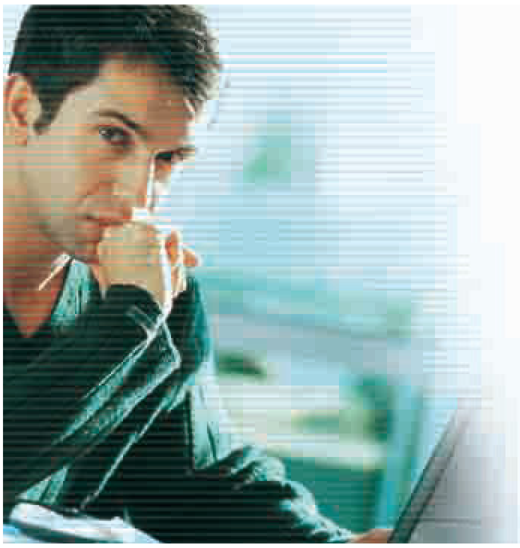
- For any reuse or distribution, you must make clear to others the licence terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the Legal Code (the full licence).

Disclaimer

JOIN THE GVIB, FOR SAFETY AND SECURITY ...



Information security has been an essential and exciting subject for many years. Almost all occupations are having to place more emphasis on the confidentiality, availability and integrity of their information. Whether you are a CISO, manager, consultant or programmer, the Information Security Practitioners Association (GvIB) can help you with information security issues.

What is the Information Security Practitioners Association?
The GvIB is an open, broad-based association for professionals to build a more professional approach to information security, through the exchange of ideas, information, knowledge, insights and above all, practical experience.

What are our aims?
We aim to promote the physical, systems and organisational security of data and data processing equipment against in-coming and outgoing breaches. We also promote the exchange of knowledge and experience and the networking of practitioners in the sector - through this Expert Letter, for example.

Our target group
The target group for the GvIB includes everyone involved in information security, either as a student or professionally, or who are especially interested in the field. Our rapidly growing membership covers many different disciplines: students, information architects, technicians, managers, organisational consultants, legal specialists, security officials and ICT auditors. Our members come from all kinds of educational backgrounds, companies, public authorities, organisations and suppliers.